Worthing Archaeological Society

Registered Charity 291431
(Affiliated to the Sussex Archaeological Society)

Worthing Archaeological Society

UK GENERAL DATA PROTECTION REGULATION (GDPR) 2018

STATEMENT OF COMPLIANCE
(Updated 23.10.22)

CONTENTS

1.	INTRODUCTION	Page 3
2.	GDPR LEGISLATION	Page 3
3.	GDPR PRINCIPLES AND ACTION TAKEN BY WAS	
3.1	Lawfulness and transparency	Page 4
3.2	Individuals' rights	Pages 5 - 7
3.3	Accountability and governance	Page 7 - 8
3.4	Data security, international transfers and breaches	Page 8 - 9
4.	CONCLUSION	Page 9

1. INTRODUCTION

GDPR came into being on 25th May 2018. Building on the Data Protection Act (1998) but with additional requirements, it relates to personal data concerning identifiable, living individuals. It is also designed to give greater control to individuals over how their data is managed. All organisations have a duty to work towards compliance. Data breaches could incur heavy fines or litigation. Improved record keeping and administrative procedures are required to aid compliance.

The WAS project team followed advice given on the Information Commissioner's Office (ICO) website in order to comply with GDPR legislation. The GDPR Self-Assessment Checklist was used in order to identify the progress to-date for WAS.

2. GDPR LEGISLATION – WAS AS DATA CONTROLLER

According to the ICO website, a Data Controller determines the purposes and means of processing personal data and a Data Processor is responsible for processing personal data on behalf of a controller. (ico.org.uk)

Article 5(1) requires that data is:

a) "Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"The Controller be responsible for, and be able to demonstrate, compliance with the principles."

3. GDPR PRINCIPLES – WORK UNDERTAKEN BY WAS

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Step 1 of 4: Lawfulness, fairness and transparency

3.1.1. Information you hold

Your business has conducted an Information Audit to map data flows.
WAS has documented what personal data is held, where it came from, who it is shared with and what is done with it.

3.1.2. Lawful Basis for processing personal data

Your business has identified the lawful basis for processing personal data and has documented it.
Member's explicit consent has been identified as being the 'Lawful Basis' for processing their personal data; there is no other way to achieve it. This is written into the WAS Privacy Notice which is published on its website.

3.1.3. Consent

Your business has reviewed how you ask for and record consent.
WAS has achieved this by supplying a Membership Form (on the website) and obtaining member's explicit consent for holding personal data. WAS also holds Trustee consents for processing personal data for application to the Charity Commission's website. All such consents are recorded on the Members Database.

Your business has systems to record and manage ongoing consent.
WAS continually reviews consents by requesting members' up-to-date details in the 2 monthly Newsletter. Members are also notified that they have the right to withdraw consent at anytime and to contact the Membership Secretary to do so.

3.1.4. Consent to process children's personal data for on-line services

If your business relies on consent to offer online services directly to children, you have systems in place to manage it.
This is not applicable as WAS does not hold any children's personal data.

3.1.5. Vital Interests

This lawful basis is very limited in scope and generally only applies to matters of life and death.
This does not apply to any data that WAS holds.

3.1.6. Legitimate Interests as lawful basis

This is often applied to fraud prevention or for marketing purposes – not applicable to WAS.

3.1.7. Registration with the Information Commissioner's Office

WAS is registered with the Information Commissioners Office and pays an annual Data Protection Fee.

Step 2 of 4: Individuals' Rights

3.2.1. Right to be informed including Privacy Notices

Your business has provided privacy notices to individuals.

WAS has a Privacy Notice which has been added to its Membership Form and also to the Membership Page on the website. This informs individuals of the reason for collecting data, the type of data collected and who shares the data. It is clear and concise.

3.2.2. Communicate the processing of children's personal data

If your business offers online services directly to children, you communicate privacy information in a way that a child understands it.

WAS does not hold any children's personal data so this does not apply.

3.2.3. Right of access

Your business has a process to recognise and respond to individuals' requests to access their personal data. This needs to be supplied within 1 calendar month. It can be requested verbally or in writing.

WAS Process is as follows:

1) *Request will go to the Membership Secretary*
2) *Who will verify the member's identity by using reasonable means*
3) *The Membership Secretary will supply the information required*

3.2.4. Right to rectification and data quality

Your business has processes to ensure that the personal data you hold remains accurate and up-to-date.

WAS Process is as follows:

1) *Members are reminded via 2 monthly Newsletters to notify the Membership Secretary of any changes they want to make to their data holdings and consents. Records will be updated accordingly.*
2) *Trustees will be asked to update their personal data on an annual basis for application to the Charity Commission website.*

3.2.5. Right to erasure (including retention and disposal)

Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it. This can be requested verbally or in writing. WAS should respond within 1 calendar month. Identification of member should be verified.

WAS Process is as follows:

1) *If requested by a member to remove personal data, the Membership Secretary will do so from all lists, electronic and paper. She will also ask other Trustees to do the same from subsets.*
2) *Personal data will be confidentially shredded and disposed of.*
3) *The WAS Field Work Health and Fitness Form, giving emergency contact information while working on site, will be disposed of after 1 year, except in circumstances where a medical condition could result in a future insurance claim. The form will then be kept securely by the Treasurer or Membership Secretary*
4) *Member's information will be deleted from the database within two years of them ceasing to be a member (as stated in the Privacy Notice).*

3.2.6. Right to restrict processing

Your business has procedures to respond to an individual's request to restrict the processing of their personal data. Requests can be verbal or in writing. Identity needs to be verified. 1 month to respond.

WAS process is as follows:

1) *Member's personal data could be requested to be only held on the main database, for communications purposes eg: for newsletters etc. and for 'need to know' basis only, other subsets should be destroyed.*
2) *Members are informed at the beginning of WAS events when photographs will be taken and they can opt out if necessary.*

3.2.7. Right of data portability

Your business has a process to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance.

WAS process is as follows:

Memory Sticks are used as a secure transference method for data.

3.2.8. Right to object

Your business has procedures to handle an individual's objection to the processing of their personal data. Request can be verbal or in writing. Identity needs to be verified. WAS must respond within 1 calendar month.

WAS process is as follows:

1) *A member can ask for their data to be deleted at any time by contacting the Membership Secretary who will deal with it accordingly.*
2) *If a member has any concerns regarding the privacy or handling of their data, they can contact the Secretary, who will contact the Membership Secretary and GDPR subgroup to deal with the matter on a 'case by case' basis. A record will be kept of such cases. (As stated on WAS Privacy Notice).*

3.2.9. Rights relating to automated decision making including profiling

Your business has identified whether any of your processing operations constitute automated decision making and have processes in place to deal with them.

WAS does not have any operations that deal with automated decision making.

Not applicable.

Step 3 of 4: Accountability and Governance

3.3.1. Your business has an appropriate data protection policy

A UK GDPR Compliance Statement has been written, ratified by WAS Trustees and posted on the website.

Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls

The data protection policies, security controls and the UK GDPR Compliance Statement are reviewed quarterly.

Your business provides data protection awareness training for all staff

Data protection awareness training will take place during WAS Committee meetings (as necessary). A UK GDPR Compliance Statement is posted on the website.

3.3.2. Data Processor Contracts

Your business has a written contract with any data processors you use.

1) ***Charity Commission and WAS*** *- WAS has a relationship with the C.C. whereby it supplies it with confidential Trustee data for the Trustee Page on C.C. website, minimal data (eg. name only) can be seen by the public.*
2) ***Insurance Company and WAS*** *– Our insurers are data processors for us. They cross check our information with the Charity Commission.*
3) ***Worthing Museum, Library and WAS*** *– WAS have contracts with these providers for the hire of rooms. The Treasurer holds these for WAS.*

3.3.3. Information Risks

Your business manages information risks in a structured way so that management understand the business impact of personal data risks and manages them effectively.

A Risk Assessment has been carried out.

3.3.4. Data Protection by Design

Your business has implemented appropriate technical and organisational measurers to integrate data protection into your processing activities.

1) *Trustees/Committee members send out Blind Carbon Copy (BCC) emails to large membership groups to protect individual contact data (this is stated in its Privacy Notice).*
2) *At events prior warning is given when photographs are taken so that individuals can opt out if needed.*
3) *WAS restricts data to 'need to know' only.*

4) *Data is held on home computers and are backed-up locally. No Cloud storage is used.*
5) *WAS Facebook page is 'Closed' and is only accessible by its members.*

3.3.5. Data protection Impact Assessments

WAS does not use systematic and extensive profiling with significant effects; or process special category or criminal offence data or use new technologies.
Not Applicable to WAS.

3.3.6. Data Protection Officers

WAS has a GDPR Sub-Group of 3 Members.

3.3.7. Management Responsibility

Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.
It is incumbent on all WAS membership to take responsibility for compliance with GDPR principles. At the A.G.M. in March, members and committee members were updated on the work that has been carried out on this subject. Members are continually referred to the website for WAS GDPR policy documents.

Step 4 of 4: Data security, international transfers and breaches

3.4.1. Security policy

Your business has an information security policy supported by appropriate security measures.
The membership database is held on the Membership Secretary's home computer which has virus protection. Any subsets are restricted to strictly 'need to know' only. No Cloud storage is used. A black locked metal box is used for conveying members' Field Work Health and Fitness Form out to dig sites. These are guarded by the supervisor on site.

3.4.2. Breach notification

Your business has effective processes to identify, report, manage and resolve any personal data breaches. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
WAS process is as follows:
These cases must be dealt with as soon as possible and the individual's identity needs to be verified. If a member has any concerns regarding the privacy or handling of their data, they can contact the Secretary, who will contact the Membership Secretary and GDPR subgroup to deal with the matter on a 'case by case' basis.

If it is suspected a breach has occurred then WAS Data Protection Officer should notify the ICO of the possible breach within 72 hours of the occurrence. The case would then be investigated internally. A record will be kept of all such cases. The member should be informed of the ICO out-come.

3.4.3. International transfers

Your business ensures adequate level of protection for any personal data processed by others on your behalf that is transferred outside the E.U.

WAS does not carry out any international business. Not applicable to WAS.

4 CONCLUSION

This is not a 'tick box' exercise, it involves the current and ongoing standard for handling personal data and as such WAS will need to continue to review its processes and ensure they are up-to-date. However, it must be remembered that any work done needs to be proportionate to its obligations and be appropriate for an organisation of its size.

According to the on-line GDPR Checklist for Controllers, WAS has achieved a Green Rating for the work it has carried out. WAS continues to be compliant with GDPR principles.

Donna Wiltshire
(WAS GDPR Sub-group)
23rd October 2022